IN THE SPECIFICATION

On page 1, please replace the paragraph beginning on line 10 with the following amended paragraph:

Theft of information processing apparatus, such as a computer system, and its components, such as its processors, add-on cards, etc., continue to plague businesses today. Although many theft prevention~~preventive~~ measures exist today, none provides a cost-effective mechanism for an organization to both deter the theft of its properties and to track their whereabouts when stolen.

On page 2, please replace the paragraph beginning on line 1 with the following amended paragraph:

Another common theft prevention~~preventive~~ mechanism involves attaching theft detection tags to the properties of an organization. Usually, only authorized personnel of the organization have~~has~~ access to special tools that can easily remove or desensitize these tags. In addition, the organization strategically places sensing devices near the exits of its physical premises. Thus, if a property of the organization, having an attached and still sensitized tag, is brought near or past the sensing device, the sensing device alerts the security personnel of the organization. However, this method is susceptible to individuals removing or desensitizing the theft detection tags, and lacks any recovery mechanism after the property leaves the organization's physical premises.

On page 5, please replace the paragraph beginning on line 12 with the following amended paragraph:

Moreover, the term “organization” broadly refers to a number of persons or groups united for a particular purpose. Some examples of an organization are, but not limited to, a family, a group, a department, a division or a company. Any property owned by an organization is referred as an “organization property”. Also throughout the following discussions, the terms, “packet” and “network packet”, are used interchangeably. Additionally, the illustrative examples of the present invention refer to some other noteworthy terms. One such term is an Internet Protocol address (hereinafter IP address), which refers to an identifier for a computer or device on a TCP/IP network. Another term “subnet” refers to a portion of a network that shares a common address component. In TCP/IP context, two devices are considered to be on the same subnet when their IP addresses have the same prefixes. Yet another term “firewall systems” refers to systems designed to prevent unauthorized users from accessing private networks. Finally, a machine readable medium refers to, but is not limited to, a storage device, a memory device, a carrier wave, etc.

On page 6, please replace the paragraph beginning on line 7 with the following amended paragraph:

Figure 1(a) illustrates a general block diagram of one embodiment of a theft prevention system that monitors organization property 102. Organization property 102 can be, but is not limited to, a desktop computer system, a notebook computer system or any electronic system owned by organization 100. The system utilizes one network configuration, which includes private network 114, firewall system 116 and outside network 118. Private network 114, as an internal network of organization 100, may operate any number of well-known or proprietary network protocols. Together with firewall system 116, private network 114 is most likely accessible only to authorized personnel of organization 100. On the other hand, outside network 118 connects organization 100 to other organizations such as third party organization 120. One example of outside network 118 is the Internet.

On page 6, please replace the paragraph beginning on line 18 with the following amended paragraph:

Moreover, this embodiment of the theft prevention system includes, but is not limited to, tamper-resistant storage 104, theft monitor 106, intranet server 110 and Internet~~internet~~ server 112. Tamper-resistant storage 104 refers to a storage medium that is difficult for unauthorized individuals to make modifications to. For instance, organization 100 may program certain information in storage devices such as a flash memory or a one-time programmable memory so that the stored information is difficult to tamper with. Alternatively, tamper-resistant storage 104 may also refer to an ordinary storage device, such as a disk driver, where one ordinarily skilled in the art opts to encrypt and store sensitive information in obscure locations of the device.

On page 7, please replace the paragraph beginning on line 8 with the following amended paragraph:

Tamper-resistant storage 104 typically stores identification information that pertains to organization 100's ownership of organization property 102. Subsequent discussions refer to this identification information as "stored identification information". Some examples of the stored identification information are, but not limited to, an IP address, subnet information, serial numbers, device identification numbers, network addresses of intranet server 110 and Internet~~internet~~ server 112, etc.

On page 7, please replace the paragraph beginning on line 14 with the following amended paragraph:

One embodiment of theft monitor 106 accesses tamper-resistant storage 104 and applies the stored identification information to authenticate the ownership of organization property 102. Specifically, theft monitor 106 first collects identification information from organization property 102. Subsequent discussions refer to this information as "collected identification information". The collected identification information not only includes the same type of information as the stored identification information, but may also comprise further information reflective of the identity of organization property 102's user or the location of organization property 102. Then theft monitor 106 compares the two types of identification information and transmits the comparison result and any other relevant identification information to intranet server 110 or Internet~~internet~~ server 112. It is important to note that one ordinarily skilled in the art may implement the described functionality of theft monitor 106 either in hardware or in software without exceeding the scope of the present invention.

On page 8, please replace the paragraph beginning on line 8 with the following amended paragraph:

Aside from this described system-level monitoring, another embodiment of a theft prevention system is capable of conducting component-level monitoring as shown in Figure 1(b). In particular, still utilizing tamper-resistant storage 104, theft monitor 106, intranet server 110 and Internet~~internet~~ server 112, this system mainly monitors organization property 102", which represents components of a system. For instance, organization property 102" can be, but is not limited to, a processor, an add-in card, etc. of electronic system 124. Also, theft monitor 106 in Figure 1(b) mainly derives the collected identification information from electronic system 124.

On page 8, please replace the paragraph beginning on line 16 with the following amended paragraph:

As shown in both Figure 1(a) and Figure 1(b), theft monitor 106 communicates with intranet server 110 and Internet~~internet~~ server 112 through network access controller 108 and 108", respectively. One ordinarily skilled in the art should note that these network access controllers provide connectivity services for various types of communication mediums, such as copper wire, lasers, microwaves, communication satellites, etc.

On page 9, please replace the paragraph beginning on line 16 with the following amended paragraph:

Although Internet~~internet~~ server 112 is also a server system, unlike intranet server 110, it avails some of its services to entities outside of firewall system 116. For instance, Internet~~internet~~ server 112 may directly receive and respond to email messages from third party organization 120. Thus, when organization property 102 or 102" detaches from private network 114 and as a result loses contact with intranet server 110, one embodiment of a theft prevention system relies on Internet~~internet~~ server 112 to relocate the property. More particularly, Internet~~internet~~ server 112 listens for information from theft monitor 106 of the property on outside network 118. Subsequent sections will present examples to elaborate on these servers' roles in a theft prevention system.

On page 12, please replace the paragraph beginning on line 4 with the following amended paragraph:

Figure 4 illustrates a flow chart of one process that one embodiment of a theft prevention system follows in response to theft scenario 1. Processor P corresponds to organization property 102" and validation system V to electronic system 124 as shown in Figure 1(b). In block 400, the theft prevention system establishes a set of parameters for monitoring properties such as processor P. These monitoring parameters may specify, but are not limited to, the amount of time for organization property 102" to remain connected to private network 114 and the type of information exchanges between intranet server 110 and theft monitor 106 of organization property 102". As an illustration, the monitoring parameters may require theft monitor 106 of processor P to transmit or cause to transmit a specifically formatted network packet to intranet server 110 periodically. This network packet contains authentication information related to processor P.

On page 12, please replace the paragraph beginning on line 16 with the following amended paragraph:

As has been discussed above, authentication of the ownership of processor P can be accomplished by comparing collected identification information and stored identification information relevant to processor P. In one implementation, tamper-resistant storage 104 contains network addresses of intranet server 110 and Internet~~internet~~ server 112 and a unique device identification information of device D. Theft monitor 106 sends requests to device D to obtain this identification information. If the collected device identification information does not match the stored one, theft monitor 106 generates a mismatched message that indicates a possible misplacement of processor P. Otherwise, theft monitor 106 generates a matched message.

On page 13, please replace the paragraph beginning on line 16 with the following amended paragraph:

Security personnel 122 are typically stationed~~stations~~ at entrances or exits of the physical premises of organization 100 and have~~has~~ limited authority to inspect employees' personal belongings. One embodiment of intranet server 110 also has capabilities of identifying a list of employees with access to the lab by accessing employee records in database 206. Intranet server 110 can present the list to security personnel 122 to thus possibly prevent the perpetrator from leaving the premises of organization 100 with processor P.

On page 14, please replace the paragraph beginning on line 3 with the following amended paragraph:

As to theft scenario 2, although the process shown in Figure 4 is applicable, one embodiment of a theft prevention system involves additional interactions among theft monitor 106, intranet server 110 and Internet~~internet~~ server 112. Figure 5 illustrates a flow chart of one process that theft monitor 106 follows to further demonstrate these interactions. Similar to the authentication process described in theft scenario 1, theft monitor 106 also authenticates the ownership of notebook computer N, which corresponds to organization property 102 as shown in Figure 1(a), by comparing appropriate collected identification information and stored identification information in block 500.

On page 14, please replace the paragraph beginning on line 12 with the following amended paragraph:

More specifically, in one implementation, tamper-resistant storage 104 contains network addresses of intranet server 110 and Internet~~internet~~ server 112 and a range of IP addresses and subnet information assigned to notebook computer N. Before the perpetrator is able to connect to the Internet through his or her ISP, or third party organization 120 as shown in Figure 1(a), another IP address has to be assigned to notebook computer N. With that in mind, theft monitor 106 searches through configuration information of N for this newly assigned IP address and collects the search outcome. Theft monitor 106 then compares the collected IP address with the information stored in tamper-resistant storage 104. If the collected IP address neither belongs to the pre-assigned subnet nor falls within the pre-assigned range of IP addresses, theft monitor 106 generates a mismatched message that indicates a possible misplacement of notebook computer N.

On page 15, please replace the paragraph beginning on line 14 with the following amended paragraph:

However, because notebook computer N is no longer on private network 114 in theft scenario 2, the intranet packet will not reach intranet server 110. After a certain amount of time has lapsed or after a certain number of attempts have been made, theft monitor assembles and transmits an Internet~~internet~~ packet with the network address of Internet~~internet~~ server 112 as the destination address in block 506. In the Internet~~internet~~ packet, theft monitor 106 may embed information representative of its failure to communicate with intranet server 110 and any relevant information indicative of the location of notebook computer N. Some examples of such relevant information are, but not limited to, the newly assigned IP address, the login name of the user, the name of the ISP, etc. Then theft monitor 106, through network access controller 108, repeatedly transmit these Internet~~internet~~ packets to Internet~~internet~~ server 112.

On page 16, please replace the paragraph beginning on line 3 with the following amended paragraph:

Although specific examples have been provided to illustrate the operations of a theft prevention system, one with ordinary skill in the art may implement the illustrated system without all the disclosed details. For example, instead of assembling either the intranet packet or the Internet~~internet~~ packet itself, the described theft monitor106 may instruct network access controller 108 or 108" to assemble the packets. An ordinarily skilled artisan may also further divide or combine the functionality of the discussed components of the theft prevention system and establish other monitoring parameters to monitor properties of an organization than the ones disclosed without exceeding the scope of the present invention.

On page 22, please replace the Abstract of the Disclosure with the following amended Abstract:

A method and apparatus for preventing theft of an organization property is disclosed. In one embodiment, the method and apparatus authenticates the ownership of an organization property by comparing stored identification information with collected identification information of the organization property. Then the method and apparatus transmits multiple types of network packets containing such authentication result to organization servers via a network.